DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-06-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/02/1998

To:	National Security	**Attn:** NIPC-CIU, Room 11887, SSA [redacted]
	Boston	**Attn:** NIPC Supervisor/Coordinator
	Charlotte	**Attn:** NIPC Supervisor/Coordinator
	Columbia	**Attn:** NIPC Supervisor/Coordinator
	Indianapolis	**Attn:** NIPC Supervisor/Coordinator
	Los Angeles	**Attn:** NIPC Supervisor/Coordinator
	Mobile	**Attn:** NIPC Supervisor/Coordinator
	Philadelphia	**Attn:** NIPC Supervisor/Coordinator
	Pittsburgh	**Attn:** NIPC Supervisor/Coordinator
	San Antonio	**Attn:** NIPC Supervisor/Coordinator
	Tampa	**Attn:** NIPC Supervisor/Coordinator

From: Cincinnati
Squad 4
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 - (Pending) 40

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ [redacted]

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

b3
OTHER Sealed Court Docume

Enclosures: (U) ~~(S)~~ [redacted]

Details: (U) ~~(S)~~ For information of recipients, captioned matter is a joint FBI/United States Air Force Office of Special Investigations (AFOSI) computer intrusions investigation. By way of brief background, FBI Cincinnati is investigating unauthorized

~~SECRET~~

288-CI-68562-40

Searched [redacted]
Serialized [redacted]
Indexed [redacted]
Filed [redacted]

337B801.EC

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 02/01/1999

To: Cincinnati **Attn:** SA [redacted]
Squad 4

National Security **Attn:** NIPC-CIU, Room 1187
SSA [redacted]

From: Columbia
Squad 7 / Greenville Resident Agency
Contact: IA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562-68 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Response to lead 40.3. [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

Enclosures: (U) ~~(S)~~ [redacted]

Details: (U) ~~(S)~~ [redacted]

♦♦

~~SECRET~~

288-CI-68562-68

RJW BJB

To: National Security From: Cincinnati
Re (U) (S) 288-CI-68562, 12/02/1998

Set Lead 1:

BOSTON

AT CAMBRIDGE, MA

(U) (S)

Set Lead 2:

CHARLOTTE

AT DURHAM, NC

(U) (S)

Set Lead 3:

COLUMBIA

AT GREENVILLE, SC

(U) (S)

b3
b6
b7C
OTHER Sealed Court Document

Set Lead 4:

INDIANAPOLIS

AT SOUTH BEND, IN

(U) (S)

To: National Security From: Cincinnati
Re: (U) ~~(S)~~ 288-CI-68562, 12/02/1998

Set Lead 5:

LOS ANGELES

AT PASADENA, CA

(U) ~~(S)~~ [redacted]

Set Lead 6:

MOBILE

AT AUBURN UNIVERSITY, AL

(U) ~~(S)~~ [redacted]

Set Lead 7:

b3
b6
b7C
OTHER Sealed Court Documents

PHILADELPHIA

AT BRYN MAWR, PA

(U) ~~(S)~~ [redacted]

Set Lead 8: (Fax) 215.641.6059

SA [redacted] FT Wash Ofc.
SSA [redacted]

AT HAVERFORD, PA

FBI Fort Washington 501 Office Center Dr. Suite 320 Fort Wash. PA 19034

(U) ~~(S)~~ [redacted]

Set Lead 9: (Fax) 610.325.6697

SA [redacted]
SSA [redacted]

~~SECRET~~

SA [redacted] Security Officer

b3
b6
b7C
OTHER Sealed Court Documents

PITTSBURGH

AT PITTSBURGH, PA

(U) ~~(S)~~ [redacted]

Set Lead 10:

SAN ANTONIO

AT AUSTIN, TX

(U) ~~(S)~~ [redacted]

Set Lead 11:

TAMPA

AT MELBOURNE, FL

(U) ~~(S)~~ [redacted]

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/10/1998

To: National Security **Attn:** NIPC-CIU, Room 11887,
SSA [redacted]

Philadelphia **Attn:** NIPC Supervisor/Coordinator
SA [redacted]
Ft. Washington RA:
SA [redacted]
Newtown Square RA

b6
b7C

From: Cincinnati
Squad 4
Contact: SA [redacted] (vm)

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562-45 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Leads set for Philadelphia Division.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

Administrative: (U) ~~(S)~~ Referenced serial serves as a brief synopsis of captioned matter. Reference telcals with Philadelphia Division NIPC Supervisor; SA [redacted] Ft. Washington RA and SA [redacted] Newtown Square RA, Pa., dated 12/16/1998.

b6
b7C

Details: (U) ~~(S)~~ As the Philadelphia Division is aware, Cincinnati Division is investigating unauthorized intrusions into computer systems located at Wright-Patterson Air Force Base (WPAFB), Dayton, Ohio.

(U) ~~(S)~~ Investigation has revealed that the unidentified intruder(s) has made numerous connections to sundry educational sites not previously seen.

288-CI-68562-45

~~SECRET~~

Searched
Serialized
Indexed
Filed

344BBOI.EC ✓

To: National Security From: Cincinnati
Re: (U) ~~(S)~~ 288-CI-68562, 12/10/1998

b3
b6
b7C
OTHER Sealed Court Documents

(U) ~~(S)~~ Investigation conducted by the Cincinnati Division and FBIHQ, NIPC-CIU Unit, has observed a multitude of past and continuous unauthorized intrusions into the computer systems at Bryn Mawr College, Haverford College and University of Pennsylvania. Based on this observation, the Philadelphia Division is requested to maintain contact with [redacted] Assistant United States Attorney (AUSA), Eastern District of Pennsylvania, and [redacted] Trap and Trace Devices and Pen Registers [redacted]

(U) ~~(S)~~ For purposes of facilitating the court orders, Cincinnati Division faxed a pony copy of an edited court order to the Philadelphia Division Resident Agencies and the AUSA in the Eastern District of Philadelphia.

b3
OTHER Sealed Court Documents

(U) ~~(S)~~ Cincinnati Division has maintained contact [redacted] trap and trace [redacted]

(U) ~~(S)~~ [redacted] Cincinnati Division will attempt to contact [redacted] to advise him of the pending court order and will furnish him with a brief synopsis of this matter.

b6
b7C

(U) Cincinnati Division appreciates the Philadelphia Division's assistance in this matter.

To: National Security From: Cincinnati
Re: (U) ~~(S)~~ 288-CI-68562, 12/10/1998

LEAD (s):

Set Lead 1:

b3
b6
b7C
OTHER Sealed Court Documents

PHILADELPHIA

AT FT WASHINGTON, PA

(U) ~~(S)~~ Maintain contact with [redacted] AUSA, Eastern District of Pennsylvania, [redacted]

Set Lead 2:

AT NEWTOWN SQUARE, PA

(U) ~~(S)~~ Maintain contact with [redacted] AUSA, Eastern District of Pennsylvania, [redacted]

Set Lead 3:

AT PHILADELPHIA, PA

(U) ~~(S)~~ Maintain contact with [redacted] AUSA, Eastern District of Pennsylvania, [redacted]

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

~~SECRET~~

Case ID: 288-CI-68562
Serial: 45

Lead 1 Set to: PHILADELPHIA

Lead 2 Set to: PHILADELPHIA

Lead 3 Set to: PHILADELPHIA

Total leads set: 3
Total leads not set: 0

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

~~SECRET~~

Date of transcription 12/18/98 b6 b7C

On 12/14/98, [redacted] date of birth [redacted] [redacted] for Harvard University Faculty of Arts and Sciences Computer Services (FAS), Science Center, 1 Oxford Street, Cambridge, MA 02138 [redacted] was interviewed at his place of business. [redacted] was advised of the nature of the interview and the identity of the interviewing agent. He provided the following information:

[redacted] advised that after having the graduate student who is responsible for the systems administration of the computer system named jsbach.harvard.edu with the IP address of 129.137.41.32, nothing suspicious was

b3 b6 b7C OTHER Sealed Court Documents

There were no suspicious logins or connections identified and no indication that the computer system had in fact been compromised. [redacted] jsbach.harvard.edu is [redacted] yoa, currently at the [redacted] b6 b7C

[redacted] advised [redacted] that there had been some activity on a Chemistry Department computer that appeared to be compromised. A report was made by a student stating that the student had found a sniffer on the computer that had caught the students password. The student notified the FAS department who administers jsbach.harvard.edu and her password was changed. There were two terminal that were suspected, one being a PC and one a Macintosh computer. After a brief investigation, it was discovered that the activity was not a compromise, but actually generated by a Harvard researcher and student from local dialup accounts. The researcher and student were working with the Dudley Hirschbach Group.

[redacted]

b3 b6 b7C OTHER Sealed Court Documents

288-CI-68562-46

Investigation on 12/14/98 at Cambridge, MA

File # 288-CI-68562-46 Date dictated [redacted]

by SA [redacted] b6 b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

sensitive. [redacted] stated that there was information on the computer system that would be sensitive to the users. Lastly, [redacted] gave an open invitation for any FBI employee interested in looking at the computer system to come to Harvard University and do so.

b6
b7C

[redacted] advised that [redacted] employs "TCP" wrappers on jsbach.harvard.edu to restrict logins. It is possible that an older user might have been able to gain access to the system through an old account and password in existence prior to [redacted] taking over the system administration for this computer system. [redacted] stated that this was highly unlikely. [redacted] also stated that it was possible that an existing user could have manipulated the computer system but again this was highly unlikely.

[redacted] stated that neither he nor [redacted] could find any sign that the computer system had been compromised. [redacted] also advised that if there were still suspicions that the Harvard staff had missed anything or if the case agent desired, [redacted] would contact his Unix specialist who could conduct extensive research into the jsbach.harvard.edu computer to attempt to identify any intrusions. At the time of the interview, [redacted] stated that he had no justification to request this type of manpower and time expenditure unless a specific compromised account could be identified or the examination was specifically requested by the FBI.

b6
b7C

According to [redacted] any activity that had been identified as suspicious, has been traced back to legitimate or explainable sources. [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/18/1998

To: Cincinnati ✓ **Attn:** ✓SA
Squad 4

From: Boston
Squad C-11
Contact: SA RJY

b6
b7C

Approved By:

Drafted By:

Case ID #: (U) ~~(S)~~ 288-CI-68562 ✓(Pending) RUC 47

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Results from lead set for Boston. Providing Cincinnati with all written and computer documentation regarding lead.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Enclosures: (U) ~~(S)~~ Provided to Cincinnati are one original and two copies of FD-302 from interview of [redacted] one copy of original EC and lead, [redacted] one original and [redacted]

Details (U) ~~(S)~~ [redacted]

b3
b3
b7C
OTHER Sealed Court Documents

(U) ~~(S)~~ The writer has included for the case agent copies of the FD-302 from [redacted]

Sec serial #57 in main file

~~SECRET~~

288-CI-68562-47

SERIALIZED FILED
DEC 1998
CINCINNATI

352 RJY 02. EC

written form. The writer is providing both this original format of questions along with an amended copy of this information containing only the pertinent information for the investigation out of Cincinnati.

b3
OTHER Sealed Court Documents

(U) ~~(S)~~ [redacted]

(U) ~~(S)~~ [redacted] of Harvard University has advised the writer that if there is any other information needed, he would be happy to provide whatever assistance he can. With the return of the previously mentioned information, the Boston Office will consider this lead covered.

b6
b7C

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/22/1998

To: Cincinnati **Attn:** Squad 4
SA [redacted]

From: Los Angeles
Squad 1/WCRA
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)-48

Title: (U) ~~(S)~~ MOONLIGHT MAZE OTHER Sealed Court Documents

Synopsis (U) ~~(S)~~ [redacted]
information.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X-1**~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

Details: (U) ~~(S)~~ [redacted]

b6
b7C
OTHER Sealed Court Documents

[redacted]

(U) ~~(S)~~ [redacted]

[redacted]

(U) ~~(S)~~ The envelope, FD-597 form (Receipt for Property Received), and FD-192 form (Control of General Evidence) are being mailed to Cincinatti under separate cover.

♦♦

288-CI-68562-48

SERIALIZED FILED

1998

[redacted] b6 b7C

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/17/98

[redacted] Office of Information Technology, Duke University, Durham, N.C. was located at his office, 3100 Tower Blvd., Suite 400 in Durham. [redacted] was advised of the official identity of the interviewing agent [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

On December 17, 1998, [redacted] was recontacted. He advised that [redacted] There are numerous computer/work stations in that department all of which use the same generic log in. The work stations at Duke are owned and managed by the University Departments, or are privately owned property of the individual graduate students working temporarily in these departments. The graduate student computers are not furnished by or purchased through Duke and there is no master work station and no oversight over any of them; each person runs his/her own work station. Further, the web pages are shared by the whole department and anyone from the department head to the cleaning lady who has "captured" the password can use any one of the computer/work stations to receive and send messages. The computer/work station involved is probably assigned to a graduate student, but the exact one can not be determined.

Further, [redacted] has determined that all of the computers in this department had their hard drives scrubbed (erased) on or about October 15, 1998.

b6
b7C

[redacted] pointed out that this is a university, and in academia, the free, open and unrestrained sharing of information is fundamental. He is quite aware that in private industry, the

Investigation on 12/14-17/97 at Durham, N.C.

File # 288-CI-68562 Date dictated 12/17/98

b6
b7C

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

government or the military, there is a much higher degree of control and accountability.

[redacted] who is [redacted] for Engineering, Experimental Electrophysiology Laboratory, Duke University, Durham, N.C. [redacted] is the person who should be contacted. A greater degree of detail will be necessary, however, to try to identify a specific computer and due to the generic structure of the University Departments, it will probably be very difficult. [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

b3
b6
b7C
OTHER Sealed Court Documents

Date of transcription 12/18/98

[redacted] Office of Legal Counsel, Duke

[redacted]

She stated Duke will provide all of the assistance possible. Should a university computer need to be seized, a subpoena/court order or search warrant should be directed to her at 2400 Pratt Street, Suite 4000, Durham, N.C. 27710. If the computer in question is identified as the private property of one of the students, then the subpoena (etc.) should be directed to the student. In that case, she would request an information copy be provided or, at least shown to, her.

[redacted] advised that it is fairly standard practice of the different departments at Duke to periodically erase or purge all of the computers in their departments at one time in order to avoid data overload and the consequent slowing down of their operation.

b6
b7C

Investigation on 12/18/98 at Durham, N.C.

File # 288-CI-68562 Date dictated 12/18/98

b6
b7C

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/29/1998

To: Cincinnati **Attn:** SA [redacted]

From: Charlotte
Raleigh/Durham RA
Contact: SA [redacted] b6 b7C

JLW/ma
Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562- 51 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Duke University able to identify department where computer data targeted by Cincinnati as their Biomedical Engineering Department. Additional identifying information required to even attempt to identify which specific computer was used and it is uncertain even that can be achieved. Any of the computers in that department can be used by anyone in that department who has access to the generic password. Additionally, all of the department's computers were scrubbed (erased) approximately October 15, 1998; a fairly standard operating procedure according to Duke's legal counsel. FD-302s of interviews with [redacted] Duke's Office of Information Technology and [redacted] Duke's Legal Counsel Office are enclosed.

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X-1~~ b6 b7C

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40, and CE telcall to CI 12/18/98.

Enclosures: (U) ~~(S)~~ Enclosed for Cincinnati are an original and six copies each of FD-302s of a) [redacted] Duke University Office of Information Technology and b) [redacted] Duke University Office of Legal Counsel and c) one 1-A envelope containing interview notes.

Details: (U) ~~(S)~~ Duke University Point of Contact, [redacted] 51

b3
b6
b7C
OTHER Sealed Court Documents

~~SECRET~~

SEARCHED INDEXED
SERIALIZED FILED
JAN 7 1999
FBI - CINCINNATI

To: Cincinnati From: Charlotte
Re: (U) ~~(S)~~ 288-CI-68562, 12/29/1998

[redacted]

b3
b6
b7C
OTHER Sealed Court Documents

[redacted] However, a copy was furnished to [redacted] of Duke's Legal Counsel Office. (Her office has a long history of excellent cooperation with the FBI and currently employs a retired SA). [redacted] will provide all possible assistance, and requested any requirement to seize a computer(s) from Duke come in the form of a subpoena/court order or search warrant directed to her (address in FD-302).

Cincinnati is requested to advise Charlotte how it wishes to proceed.

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 12/23/1998

To: National Security Attn: NIPC-CIU, Room 11887,
SSA
Cincinnati Attn: SA

From: Philadelphia
Ft. Washington RA
Contact: SA

Approved By:

Drafted By:

Case ID #: 288-CI-68562-52 (Pending)

Title: MOONLIGHT MAZE

Synopsis: Results of lead to Philadelphia Division, Ft. Washington RA, Point of Contact (POC).

Reference: 288-CI-68562 Serial 40

Details: On 12/22/98, Assistant United States Attorney (AUSA) Eastern District of Pennsylvania (EDPA), sent by facsimile

advised that the Computing Services Department, and all other departments at the college, would close at 2:00 p.m. on 12/23/98 and reopen at 8:00 a.m. on 1/4/99.

SA Cincinnati Division, was advised of the above information in a telephone call on 12/23/98.

SSA FBI Academy, ERS, and SSA Tech Squad, Philadelphia Division, contacted writer on 12/23/98,

~~SECRET~~

~~UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES~~

288-CI-68562-52

SEARCHED INDEXED
SERIALIZED FILED
JAN 18 1999
FBI — CINCINNATI

To: Cincinnati From: Philadelphia
Re: 288-CI-68562, 12/23/1998

b3
b6
b7C
OTHER Sealed Court Documents

♦♦

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 01/08/1999

To: National Security **Attn:** NIPC-CIU, Room 11887,
SSA [redacted]

From: Cincinnati
Squad 4
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID # (U) ~~(S)~~ 288-CI-68562 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Update concerning captioned matter.

(U) ~~(S)~~ ~~**Derived From : G-3**~~
~~**Declassify On: X1**~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 45

Administrative: (U) ~~(S)~~ Reference telcall between SSA [redacted] NIPC-CIU, FBIHQ and SA [redacted] FBI Cincinnati, dated 01/06/1999.

b6
b7C

Details: (U) ~~(S)~~ Instant communication serves to formally advise NIPC-CIU the following updated information concerning captioned matter:

(U) ~~(S)~~ On 01/06/99, [redacted] Engineering Research Facility (ERF), Quantico, Va., [redacted] trap and trace and pen registers [redacted]

b3
b6
b7C

(U) ~~(S)~~ [redacted] trap and trace/pen register [redacted] trap and trace/pen register [redacted] trap and trace/pen registers [redacted]

~~SECRET~~

288-CI-68562-53

Serialized [redacted]
Indexed [redacted]
Filed [redacted]

0076501.ec ✓

To: National Security From: Cincinnati
Re: (U) ~~(S)~~ 288-CI-68562, 01/08/1999

[redacted]

b3
b6
b7C

(U) ~~(S)~~ The trap and trace/pen registers [redacted]

[redacted]

(U) ~~(S)~~ For the information of the NIPC-CIU unit, Cincinnati Division is awaiting official copies of the trap and trace/pen register court orders from the U.S. Attorney's office in Philadelphia. As soon as they are received in Cincinnati, Cincinnati will expeditiously facsimile the copies to NIPC-CIU unit.

♦♦

(01/26/1998)

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY Date: 01/08/1999

To: Cincinnati Attn: Squad 4
SA [redacted]

National Security Attn: NIPC-CIU, Room 11887,
SSA [redacted]

From: Philadelphia
Squad 9
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562 -54 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ Trap and Trace Devices and Pen Register [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 45

Details: (U) ~~(S)~~ Trap and Trace / Pen Register [redacted] Details for each are as follows.

(U) ~~(S)~~ [redacted]

(U) ~~(S)~~ [redacted]

~~SECRET~~

288-CI-68562 -54

SEARCHED _____ INDEXED _____
SERIALIZED _____ FILED _____
JAN 14 1999
FBI — CINCINNATI

To: Cincinnati From: Philadelphia
Re: (U) ~~(S)~~ 288-CI-68562, 01/08/1999

[redacted]

(U) ~~(S)~~ [redacted]

[redacted]

b3
b6
b7C

(U) ~~(S)~~ [redacted]

[redacted]

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/08/99 Time: 13:47

Case ID: 288-CI-68562 Serial: 55

Description of Document:

Type : FD302
Date : 12/14/98
To : CINCINNATI
From : CHARLOTTE
Topic: [redacted]

Reason for Permanent Charge-Out:

SERIAL 49 IS THE SAME SERIAL

Employee: [redacted]

b6
b7C

288-CI-68562-55

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/08/99 Time: 13:48

Case ID: 288-CI-68562 Serial: 56

Description of Document:

Type : FD302
Date : 12/18/98
To : CINCINNATI
From : CHARLOTTE
Topic: [redacted]

Reason for Permanent Charge-Out:

SERIAL 50 IS THE SAME SERIAL

Employee: [redacted]

b6
b7C

288-CI-68562-56

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/11/1999

[redacted] of Academic and Research Computing Services, Florida Institute of Technology (FIT), 150 West University Boulevard, Melbourne, Florida, telephone [redacted] was contacted at her place of employment.

b6
b7C

[redacted] On December 14, 1998, the investigating agent met at her office located on the FIT campus. [redacted] was advised of the identity of the investigating agent and the purpose of the investigation.

[redacted]

b3
b6
b7C
OTHER Sealed Court Documents

Investigation on 1/11/1999 at Melbourne, Florida

File # 288-CI-68562 -58 Date dictated 1/11/1999

b6
b7C

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 01/11/1999

To: Cincinnati **Attn:** SA [redacted]
Squad 4

From: Tampa
Squad 6/Brevard RA
Contact: [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562 (Pending) - 59

Title: MOONLIGHT MAZE

Synopsis: Investigation at Florida Institute of Technology.

Reference: 288-CI-68562 Serial 40

Enclosures: Enclosed for CI is the original and two copies of an FD-302 reflecting investigation at the Florida Institute of Technology, and an FD-340 containing computer logs.

Details: [redacted] b3 b6 b7C

OTHER Sealed Court Documents [redacted]

288-CI-68562-59

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted] b6 b7C
JAN 19 1999
FBI — CINCINNATI

No further investigation is pending in captioned matter at Tampa Division. Accordingly, this lead is considered covered.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FACSIMILE COVER SHEET

FORT WASHINGTON RESIDENT AGENCY
501 Office Center Drive
Suite 320
Fort Washington, PA 19034

PRECEDENCE X Immediate ___ Priority ___ Routine

CLASSIFICATION ___ Top Secret ___ Secret ___ Confidential ___ Sensitive ___ Unclassified

TIME TRANSMITTED: 2:10 p.m. NUMBER OF PAGES: 5 (including cover sheet)

To: Cincinnati (Name of Office) Date: 1/6/99

Attn: SA [redacted] (Name) Fax Number: 513-562-5650

Subject: Moonlight Maze

b6
b7C

Special Handling Instructions: Contact SA [redacted] ASAP

From: SA [redacted] Fort Washington Resident Agency Telephone Number: 215-641-8910

FWRA Fax Number: 215-641-6059

288-CI-68562-60

SEARCHED ___ INDEXED ___
SERIALIZED ___ FILED ___
JAN 07 1999
FBI — CINCINNATI

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

SERIALIZED FILED
FEB 3 1999
FBI - CINCINNATI

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY Date: 01/27/1999

To: National Security Attn: NIPC- Room 11887
SSA [redacted]

Cincinnati Attn: Sq. 4,
SA [redacted]

From: Philadelphia
Ft. Washington RA
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562-64 (Pending)

Title: (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ [redacted]

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

b3
OTHER Sealed Court Documents

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 40

Package Copy: (U) ~~(S)~~ Being forwarded under separate cover to the Cincinnati Division are the following items:

[redacted]

Details: (U) ~~(S)~~ The above information was provided to SA [redacted] Philadelphia Division, Ft. Washington Resident Agency, [redacted]

~~SECRET~~

[redacted]

288-CI-68562-14
SEARCHED INDEXED
SERIALIZED FILED
FEB 3 1999
FBI - CINCINNATI
RDW/WRP

b6
b7C

by [redacted] Computing and Information Services, and [redacted] Computing and Information Services, Bryn Mawr College, Bryn Mawr, PA. 19010, telephone [redacted] This information was provided to SA [redacted] on January 26, 1999.

b6
b7C

(U) (~~S~~) [redacted] advised that two others at the college assisted in obtaining the information provided. They are [redacted] Both individuals are in the Computing and Information Services department and work for [redacted]

(U) (~~S~~) [redacted] further advised that she and [redacted] went to their legal counsel at the college for his approval in complying with the court order.

(U) (~~S~~) [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

DECLASSIFIED BY 60324/UC/baw/sab/aio
ON 07-09-2012

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY Date: 01/27/1999

To: National Security Attn: SSA [redacted] NIPC-CIU
Room 11887

Cincinnati Attn: SA [redacted]
Sq. 4

From: Philadelphia
Ft. Washington RA
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 288-CI-68562-65 (Pending)

Title (U) ~~(S)~~ MOONLIGHT MAZE

Synopsis: (U) ~~(S)~~ [redacted]

b3

(U) ~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) ~~(S)~~ 288-CI-68562 Serial 45

Administrative: (U) ~~(S)~~ Telephone call to SA [redacted] from [redacted] Engineering Research Facility (ERF), FBI Academy, Quantico, Va. on 1/15/99.

Package Copy: (U) ~~(S)~~ Being forwarded under separate cover to Cincinnati Division is an FD-540b [redacted]

b3
b6
b7C

Details: (U) ~~(S)~~ On January 15, 1999, SA [redacted] received a telephone call from [redacted] NIPC,

[redacted]

[redacted]

~~SECRET~~

288-CI-68562-65
SEARCHED [redacted] INDEXED
SERIALIZED [redacted] FILED
FBI — CINCINNATI
RSW/NEP

b6
b7C

To: National Security From: Philadelphia
Re: (U) (S) 288-CI-68562, 01/27/1999

[redacted]

Per the point of contact (POC) and technically trained agent, SA [redacted] the Philadelphia Division [redacted]

b3
b6
b7C

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/01/1999

To: Cincinnati

From: Columbia
Squad 7 / Greenville Resident Agency
Contact: IA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-CI-68562-Late (Pending)

Title: MOONLIGHT MAZE

Synopsis: Late submission of evidence.

Details: This evidence is being submitted late because writer was unaware Cincinnati required documents to be entered into evidence.

♦♦

[redacted]

RDW/BB

288-CI-68562-66

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/01/99

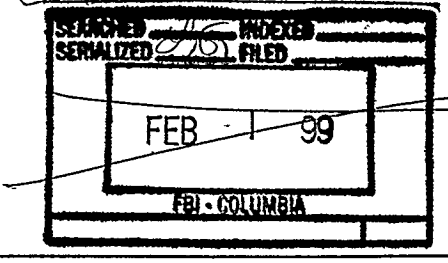
[redacted] of Information Services, Furman University, work address, 3300 Poinsett Highway, Greenville, South Carolina 29613-4904, telephone number [redacted]

b3
b6
b7C
OTHER Sealed Court Documents

[redacted] at his place of employment, Greenville, South [redacted] the below named Investigative Analyst.

[redacted]

288-CI-68562-67



Investigation on 12/23/1998 at Greenville, SC 288-CI-68562-67

File # 288-CI-68562 Date dictated 02/01/1999

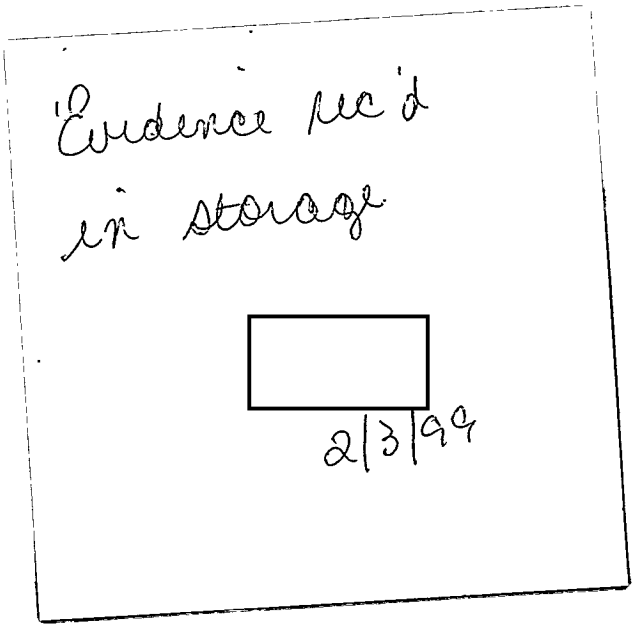
b6
b7C

by IA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

RDW/BB

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-09-2012 BY 60324/UC/baw/sab/aio



b6
b7C

intrusions into computer systems located at Wright-Patterson Air Force Base (WPAFB), Dayton, Ohio. The intrusions appear to be originating from Russia, hopping through the University of Cincinnati (UC), Cincinnati, Ohio, then terminating at WPAFB. The unknown intruder(s) has transferred several sensitive, though not classified, files to Russia. The transferred files generally are word processing and/or power point presentations dealing with cockpit design and computer chip schema.

(U) (S) Investigation has revealed that the unknown intruder(s) has made connections to various other educational sites not previously seen.

b3
OTHER Sealed Court Documents

(U) (S) Recipient Field Offices should ensure that the respective network systems administrators from the educational sites in their Division are informed that once the data from their compromised systems has been analyzed and compared to data from other compromised systems, the FBI may request additional assistance in furtherance of this investigation.

b3
OTHER Sealed Court Document

(U) (S) A Chain of Custody form should be included with the original evidence. Any and all original FD-302 interviews conducted with network systems administrators should be forwarded to FBI Cincinnati, and a copy to FBIHQ-NIPC. FBI Cincinnati will forward the original evidence to the District of Columbia Forensic Laboratory (DCFL), Bolling AFB, Washington, D.C., for analysis. DCFL will promptly return all original evidence to FBI Cincinnati for proper storage.